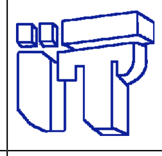
	**Manual de configuración router Linksys WRT54GS/GL UC3M**	
Departamento de Ingeniería Telemática - UC3M		2011-2012
Versión: 2011-09-22		

1. INTRODUCCIÓN

El router Linksys WRT54GS/GL es un router orientado al entorno doméstico y de pequeña empresa, que dispone de 5 interfaces Ethernet y una interfaz inalámbrica (IEEE 802.11b/g):

- Interfaces Ethernet. Tal y como se aprecia en la Figura 2, hay una primera boca (de izquierda a derecha), etiquetada como 'Internet' en el router, que internamente recibe el nombre de `eth0.0`. A continuación hay 4 bocas más, etiquetadas de 1 a 4 en el router, que internamente reciben el nombre de `eth0.1, ..., eth0.4`. Inicialmente (por defecto, después de arrancar) estas interfaces tienen configuradas las siguientes direcciones IP:
    - `eth0.0`: 192.168.0.1/24
    - `eth0.1`: 192.168.1.1/24
    - `eth0.2`: 192.168.2.1/24
    - `eth0.3`: 192.168.3.1/24
    - `eth0.4`: 192.168.4.1/24
- Interfaz inalámbrica (WLAN). Internamente recibe el nombre de `wlan0`. Inicialmente esta interfaz tiene la siguiente dirección IP:
    - `wlan0`: 192.168.5.1/24

Tenga en cuenta que para determinadas prácticas, puede ser conveniente que borre las direcciones IP configuradas por defecto después de añadir las que necesite para la realización de la práctica.





Figura 1: Vista frontal WRT54GS/GL

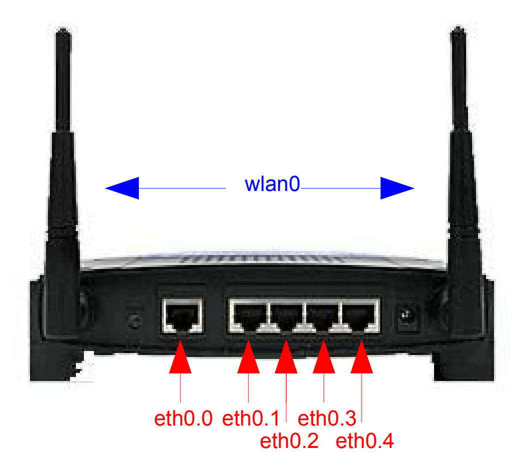


Figura 2: Vista posterior WRT54GS/GL

El router ejecuta Linux como Sistema Operativo, lo cual permite instalar en él multitud de aplicaciones y utilidades diferentes. Para las prácticas del Departamento de Ingeniería Telemática, se ha instalado software[1] que permite configurar diversas características del router y experimentar aspectos de

[1] Básicamente, se ha instalado el demonio de encaminamiento *Quagga* [1], el cual proporciona una interfaz de configuración estándar, prácticamente idéntica a la que proporciona la mayoría de routers comerciales actuales. Adicionalmente, se han instalado una serie de utilidades que permiten configurar los parámetros de la interfaz inalámbrica del router.

configuración de routers, de forma muy similar a como se hace con routers comerciales de mayor envergadura. Existen 2 maneras complementarias de acceder al router:

- Mediante *TELNET* (a cualquiera de las direcciones IP que tiene configurado el router), accediendo a una consola del router[2]. A través de dicha consola se pueden configurar todos los parámetros relacionados con interfaces (habilitar y deshabilitar interfaces), IP (direcciones, rutas estáticas) y protocolos de encaminamiento dinámicos (RIP, OSPF y BGP).
- Mediante *SSH*, accediendo a una consola Linux. Dicha consola proporciona los comandos básicos que se pueden encontrar en un sistema Linux. Este modo de acceso al router se emplea básicamente para la configuración de la interfaz inalámbrica. Los parámetros de acceso necesarios son:
  - Usuario: alumno
  - Contraseña: alumno13

Dependiendo del tipo de práctica, el alumno tendrá que utilizar uno u otro tipo (o incluso ambos en algunas ocasiones) de acceso para configurar el router. Su profesor de prácticas le indicará qué mecanismo debe emplear en cada práctica. Las primeras secciones de este manual se centran en el primer modo de acceso (a través de *TELNET*). La última sección (Sección 4) describe las posibilidades de configuración disponibles cuando se accede por SSH.

La configuración por defecto del router se restaura cada vez que se inicia el router. Por lo tanto, **todos los cambios que realice se pierden si resetea, o apaga y enciende el router**. Se recomienda **copie y pegue todos los comandos que introduce en el router en un fichero de texto**, de forma que pueda reconfigurar un router tan sólo copiando de nuevo los comandos del fichero y pegarlos en la consola de configuración del router. Esto es especialmente útil en aquellas prácticas que se realizan en varias sesiones, en las cuales en cada sesión tiene que empezar de nuevo o para restaurar aquellas partes de la configuración del router que son comunes en prácticas diferentes.

2. COMANDOS BÁSICOS

Esta sección incluye los comandos básicos de configuración que se pueden realizar a través de la consola de configuración accesible mediante un *telnet* al router. Para ello, debe configurar en su PC una dirección IP que le permita tener conectividad con el router WRT54GS/GL (la dirección dependerá de la interfaz de red del router que vaya a utilizar para acceder desde el PC). Una vez configurado el PC adecuadamente, conectado el cableado necesario, y encendido el router (el router necesita algunos segundos para arrancar, tiempo durante el cual no se puede acceder al mismo), podemos realizar un *telnet* desde el PC:

```
telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

Router UC3M IT de prácticas (versión 3)
Hello, this is Quagga (version 0.98.6).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
Adaptado por Carlos J. Bernardos <cjbc@it.uc3m.es>

routerUC3M#
```

Cuando aparece el *prompt* “`routerUC3M#`” significa que hemos accedido a la consola del router (modo terminal). Desde esta consola inicial podemos realizar diferentes acciones en el router. Para averiguar los comandos disponibles (en este y en cualquier otro modo del router), podemos teclear “`?`”:

```
routerUC3M#  ?
  clear        Reset functions
  configure    Configuration from vty interface
  copy         Copy from one file to another
  debug        Debugging functions (see also 'undebug')
```

[2] Esta consola suele recibir el nombre de CLI (*Command Line Interface*), es decir, Interfaz de Línea de Comandos.

```
  disable     Turn off privileged mode command
  end         End current mode and change to enable mode
  exit        Exit current mode and down to previous mode
  list        Print command list
  no          Negate a command or set its defaults
  ping        Send echo messages
  quit        Exit current mode and down to previous mode
  show        Show running system information
  ssh         Open an ssh connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
  undebug     Disable debugging functions (see also 'debug')
  write       Write running configuration to memory, network, or
terminal
routerUC3M#
```

Como se puede apreciar, existen multitud de posibles comandos accesibles desde este modo. Algunos de ellos además reciben parámetros adicionales que modifican su comportamiento. Al igual que antes, podemos hacer uso de "?" después de un comando dado para obtener más información sobre los parámetros que puede recibir y para qué sirven. Por ejemplo, tecleando "`ping ?`" desde este modo, obtenemos información acerca de los parámetros que puede recibir el comando *ping* (en este caso, la dirección o nombre destino al que hacer un ping y adicionalmente, si queremos hacer un *ping* utilizando el protocolo IPv4 o IPv6) :

```
routerUC3M# ping ?
  WORD  Ping destination address or hostname
  ip    IP echo
  ipv6  IPv6 echo
routerUC3M# ping
```

De todos los comandos listados anteriormente, es interesante describir los siguientes[3]:

- `configure terminal`
  - Cambia al modo de configuración. Este comando es el primer paso para configurar cualquier parámetro en el router:
    ```
    routerUC3M# configure terminal
    router(config)#
    ```

  Nótese que el *prompt* del router cambia a `router(config)#`al pasar al modo de configuración del router.
- `list`
  - Lista todos los posibles comandos que se puede ejecutar desde este modo. Esta lista muestra los comandos completos, incluyendo las posibles modificadores.
- `ping DESTINO`
  - Lanza un *ping* a la dirección IP o nombre que se le proporcione como parámetro. Admite un modificador delante del destino para especificar si éste es IPv4 (`ip`) o IPv6 (`ipv6`).
- `show`
  - Muestra información sobre la configuración actual del router. Este parámetro admite múltiples modificadores adicionales, que permiten especificar la información particular que se desea obtener. Como ejemplo de funcionamiento (utilice "?" para averiguar todas las posibilidades que ofrece este comando), el siguiente comando permite obtener información sobre una interfaz de red:
    ```
    routerUC3M# show interface eth0.1
    Interface eth0.1 is up, line protocol detection is disabled
      index 5 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,PROMISC,MULTICAST>
      HWaddr: 00:14:bf:d1:eb:07
      inet 192.168.1.1/24 broadcast 192.168.1.255
      inet6 fe80::214:bfff:fed1:eb07/64
        input packets 667, bytes 44806, dropped 0, multicast packets 8
        input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    ```

[3] Existen también otros comandos muy útiles, específicos de algunos protocolos. La utilización de dichos comandos se describe (en caso de ser necesario) en las secciones referentes a cada uno de los protocolos en particular.

```
output packets 337, bytes 30765, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

- `traceroute`
  - Lanza un *traceroute* a la dirección IP o nombre que se le proporcione como parámetro. Admite un modificador delante del destino para especificar si éste es IPv4 (`ip`) o IPv6 (`ipv6`).

Dentro de la consola del router (CLI), se pueden utilizar los siguientes comandos de movimiento (nótese que el carácter <C> significa mantener apretada la tecla Ctrl, Control):

- C-f o <CURSOR DERECHA>
  - Mueve hacia delante un carácter
- C-b o <CURSOR IZQUIERDA>
  - Mueve hacia atrás un carácter
- M-f
  - Desplaza el cursor hacia delante una palabra
- M-b
  - Desplaza el cursor hacia atrás una palabra
- C-a
  - Desplaza el cursor al inicio de la línea
- C-e
  - Desplaza el cursor al final de la línea
- C-c
  - Interrumpe la entrada actual y se mueve a la siguiente línea
- C-z
  - Finaliza la configuración actual y se mueve al nodo inicial
- C-n o <CURSOR ABAJO>
  - Se desplaza a la siguiente línea en el *buffer* del historial
- C-p o <CURSOR ARRIBA>
  - Se desplaza a la línea anterior en el *buffer* del historial
- <TAB>
  - Completa la línea pulsando sobre la tecla de tabulación

A continuación, se describen los comandos de configuración más importantes. Como regla general, para deshacer/eliminar la configuración de un comando en particular, se debe anteponer "`no`" a dicho comando (en las siguientes secciones, se muestran ejemplos de uso).

2.1 Comandos de interfaz

A partir del modo de configuración del router (recuerde que para acceder a él, tiene que teclear `configure terminal` desde la consola inicial), se puede acceder al sub-menú de configuración de interfaz de red, tecleando `interface NOMBRE_DE_LA_INTERFAZ_DE_RED`. Por ejemplo, para acceder a la configuración de la interfaz `eth0.1`, es necesario introducir el siguiente comando (desde el modo de configuración):

```
router(config)# interface eth0.1
```

Dentro del sub-menú de configuración de interfaz de red, están disponibles los siguientes comandos:

- `shutdown`
  - Deshabilita el interfaz (en el interfaz actual).
- `no shutdown`
  - Habilita el interfaz (en el interfaz actual).
- `ip address DIRECCIÓN/LONGITUD_PREFIJO`
  - Configura (añade) la dirección IP en la interfaz actual.
- `no ip address DIRECCIÓN/LONGITUD_PREFIJO`
  - Elimina la dirección IP en la interfaz actual.
- `ip address DIRECCIÓN/LONGITUD_PREFIJO secondary`
  - Configura (añade) la dirección IP como secundaria. Esto causa que OSPF no trate la dirección como de distinta subred.
- `no ip address DIRECCIÓN/LONGITUD_PREFIJO secondary`

    - Elimina la dirección IP secundaria.
- ipv6 address DIRECCIÓN/LONGITUD_PREFIJO
    - Configura (añade) la dirección IPv6 en la interfaz actual.
- no ipv6 address DIRECCIÓN/LONGITUD_PREFIJO
    - Elimina la dirección IPv6 en la interfaz actual.
- description DESCRIPCIÓN ...
    - Configura la descripción de la interfaz actual.
- no description
    - Elimina la descripción de la interfaz actual.
- multicast
    - Habilita el *flag* multicast de la interfaz actual.
- no multicast
    - Deshabilita el *flag* multicast de la interfaz actual.
- bandwidth <1-10000000>
    - Configura el ancho de banda de la interfaz actual. Este parámetro se tiene en cuanta para calcular el coste en OSPF. Este comando no modifica la configuración de la interfaz física.
- no bandwidth <1-10000000>
- exit / quit
    - Sale del sub-menú de configuración de interfaz y vuelve al menú anterior.
- no ipv6 nd suppress-ra
    - Habilita el envío de *Router Advertisements* en el interfaz.
- ipv6 nd suppress-ra
    - Deshabilita el envío de *Router Advertisements* en el interfaz.
- ipv6 nd prefix ipv6prefix
    - Configura el prefijo IPv6 que se incluirá en los Router Advertisements. Existen diversos parámetros opcionales que se pueden indicar a continuación en la misma línea del comando.
- ipv6 nd prefix ipv6prefix [valid-lifetime] [preferred-lifetime] [off-link] [no-autoconfig]
        - *valid-lifetime*: tiempo en segundos durante el cual el prefijo es válido (para el propósito de determinar si el prefijo es *on-link*). El valor 4294967295 (0xffffffff) representa infinito. También se puede indicar tiempo infinito con la palabra infinite.
        - *preferred-lifetime*: tiempo en segundos durante el cual se prefiere la dirección generada a partir del prefijo anunciado.
        - *off-link*: el anuncio no indica nada sobre las propiedades on-link u off-link del prefijo.
        - *no-autoconfig*: indica a los host del enlace que el prefijo IPv6 incluido en el anuncio no se puede utilizar para autoconfiguración IPv6.
- ipv6 nd ra-interval SEGUNDOS
    - Especifica el tiempo máximo (SEGUNDOS) permitido en segundos entre envíos de mensajes *Router Advertisement* multicast no solicitados. No puede ser inferior a 3 segundos. El valor por defecto es 600.
- no ipv6 nd ra-interval
    - Resetea el intervalo entre envíos al valor por defecto.
- ipv6 nd ra-lifetime SEGUNDOS
- no ipv6 nd ra-lifetime
    - Especifica el valor (SEGUNDOS) a incluir en el campo *Router Lifetime* de los Router Advertisements, en segundos. Este valor indica el tiempo durante el cual el router se puede utilizar como router por defecto. Un valor igual a cero indica que el router no puede utilizarse como router por defecto en esa interfaz. SEGUNDOS tiene que ser igual a cero o un valor entre el valor especificado mediante ipv6 nd ra-interval y 9000 segundos. El valor por defecto es 1800.
    - Resetea al valor por defecto.
- ipv6 nd reachable-time MILISEGUNDOS
    - Especifica el valor (MILISEGUNDOS) a incluir en el campo *Reachable Time* de los Router Advertisements, en milisegundos. Un valor igual a cero indica que el router no especifica ningún valor. MILISEGUNDOS no puede ser mayor que 3600000 milisegundos. El valor por defecto es 0.
- no ipv6 nd reachable-time
    - Resetea el intervalo entre envíos al valor por defecto.
- ipv6 nd managed-config-flag
    - Habilita el flag en los Router Advertisements que indica que los hosts deben usar un protocolo *stateful* para la configuración de direcciones, además de las direcciones que haya configurado empleando autoconfiguración *stateless*.

- `no ipv6 nd managed-config-flag`
  - Deshabilita el flag anterior en los Router Advertisements.
- `ipv6 nd other-config-flag`
  - Habilita el flag en los Router Advertisements que indica que los hosts deben usar un protocolo *stateful* para la configuración de otros parámetros diferentes a las direcciones.
- `no ipv6 nd other-config-flag`
  - Deshabilita el flag anterior en los Router Advertisements.

El modo terminal (el modo inicial de la consola del router, identificado con el *prompt* "`routerUC3M#`"), permite obtener información sobre la configuración actual de una interfaz determinada. Para ello, se utiliza el siguiente comando:

- `show interface NOMBRE_DE_LA_INTERFAZ_DE_RED`
  - Muestra información sobre la configuración actual de la interfaz proporcionada (`NOMBRE_DE_LA_INTERFAZ_DE_RED`). Si se omite el nombre de la interfaz (`NOMBRE_DE_LA_INTERFAZ_DE_RED`), el comando devuelve la información de todas las interfaces del equipo. Ejemplo:

```
routerUC3M# show interface eth0.1
Interface eth0.1 is up, line protocol detection is disabled
  index 5 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,PROMISC,MULTICAST>
  HWaddr: 00:14:bf:d1:eb:4f
  inet 192.168.1.1/24 broadcast 192.168.1.255
  inet6 fe80::214:bfff:fed1:eb4f/64
  inet6 fd33:3333:3333::1/64
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 7, bytes 674, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

2.2 Comandos de configuración de rutas IP estáticas

En el modo de configuración del router (recuerde que para acceder a él, tiene que teclear `configure terminal` desde la consola inicial), se pueden configurar rutas IP estáticas. A continuación mostramos algunos ejemplos de configuración de rutas IP estáticas:

- `ip route RED SIGUIENTE_SALTO`
  - Configura (añade) una ruta a la red de destino `RED` (con formato `A.B.C.D/M`) a través del siguiente salto `SIGUIENTE_SALTO`. `SIGUIENTE_SALTO` puede ser la dirección IP del siguiente salto (con formato `A.B.C.D`) o el nombre de la interfaz de salida[4] (en caso de que la red destino esté directamente conectada). Ejemplos:

```
router(config)# ip route 10.0.0.0/8 192.168.0.4
router(config)# ip route 10.0.0.0/8 eth0.2
router(config)# ip route 10.0.0.0/8 null0
```

- `ip route DESTINO MÁSCARA SIGUIENTE_SALTO`
  - Comando idéntico al anterior, pero utilizando el `DESTINO` (con formato `A.B.C.D`) `MÁSCARA` (con formato `A.B.C.D`), en vez de `RED` (que indica la longitud del prefijo). Ejemplos:

```
router(config)# ip route 10.0.0.0 255.0.0.0 192.168.0.4
router(config)# ip route 255.0.0.0 eth0.2
router(config)# ip route 10.0.0.0 255.0.0.0 null0
```

- `ip route RED SIGUIENTE_SALTO DISTANCIA /`
  `ip route DESTINO MÁSCARA SIGUIENTE_SALTO DISTANCIA`
  - Configura (añade) una ruta con la distancia especificada en `DISTANCIA`.
- `ip route RED {blackhole/reject} /`
  `ip route DESTINO MÁSCARA {blackhole/reject}`
  - Adicionalmente, se puede configurar el router para que descarte paquetes hacia un destino, especificando el comportamiento del router cuando descarta dichos paquetes:
    - `blackhole`: el router descarta silenciosamente los paquetes.

[4] Si se utiliza la interfaz `null0`, la ruta se instala como inalcanzable.

    - ◆ `reject`: el router descarta los paquetes y envía un mensaje ICMP de destino inalcanzable (Destination Host Unreachable).
- `ipv6 route RED SIGUIENTE_SALTO`
    - Configura (añade) una ruta IPv6 a la red de destino `RED` (con formato `PREFIJO/M`) a través del siguiente salto `SIGUIENTE_SALTO`. `SIGUIENTE_SALTO` puede ser la dirección IP del siguiente salto o el nombre de la interfaz de salida[5] (en caso de que la red destino esté directamente conectada). Al igual que en el comando para Ipv4, se pueden especificar parámetros adicionales, como la distancia administrativa, etc. Adicionalmente, también se puede especificar la interfaz de salida (necesario por ejemplo si se emplean direcciones de tipo link-local como siguiente salto).

Para borrar una ruta configurada en el router, basta con anteponer "`no`" al comando (de los anteriormente descritos) que emplearía para crear la ruta.

Para añadir rutas IPv6 estáticas, la sintaxis es la misma que la descrita anteriormente para IPv4, con la diferencia de que los comandos tienen la forma "`ipv6 route ...`" en lugar de "`ip route ...`".

El modo terminal (el modo inicial de la consola del router, identificado con el *prompt* "`routerUC3M#`"), permite obtener información sobre las rutas configuradas en el router (independientemente de que se hayan configurado estáticamente o mediante un protocolo de encaminamiento). Para ello, se utiliza el siguiente comando:

- `show ip route`
    - Muestra las rutas que el router tiene actualmente configuradas, mostrando información sobre el origen de la ruta. Por ejemplo:

```
routerUC3M# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O – OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route
R>* 10.0.0.0/24 [120/8] via 10.0.2.173, eth0.4, 2d03h03m
R>* 10.0.2.0/26 [120/8] via 10.0.2.166, eth0.3, 2d03h03m
R>* 10.0.2.64/26 [120/8] via 10.0.2.170, eth0.2, 2d03h03m
C>* 10.0.2.128/27 is directly connected, eth0.1
R>* 10.0.2.160/30 [120/8] via 10.0.2.166, eth0.3, 2d03h03m
C>* 10.0.2.164/30 is directly connected, eth0.3
C>* 10.0.2.168/30 is directly connected, eth0.2
C>* 10.0.2.172/30 is directly connected, eth0.4
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.0.0/24 is directly connected, eth0.0
R>* 192.168.4.0/24 [120/8] via 10.0.2.166, eth0.3, 2d03h03m
C>* 192.168.5.0/24 is directly connected, wlan0
```

    Nótese que las primeras líneas de la salida que devuelve el comando incluyen una pequeña leyenda explicativa sobre unos códigos que se anteponen a cada entrada de la tabla de rutas. Estos códigos proporcionan información acerca del origen de las entradas en la tabla de encaminamiento: "C" para rutas directamente conectadas, "S" para rutas estáticas, "R" para rutas aprendidas por RIP, "O" para rutas obtenidas por OSPF, "K" para rutas configuradas por el kernel del sistema operativo, etc... El símbolo "*" implica que la ruta está en la *Forwarding Information Base* (FIB), es decir la tabla de rutas que utiliza el equipo a la hora de encaminar. Esto es útil para determinar cuál(es) de las posibles rutas que puede tener el router para un mismo destino está siendo utilizada para encaminar el tráfico. Otra información útil que muestra este comando es la distancia administrativa y la métrica de las rutas, utilizando el siguiente formato `[DISTANCIA_ADMINISTRATIVA, MÉTRICA]` (si la distancia administrativa es 0 – lo cuál implica que se trata de una ruta directamente conectada – esta información no se muestra).

    - El comando acepta parámetros adicionales, que permiten filtrar la salida/obtener información específica sobre determinado tipo de rutas:

```
routerUC3M# show ip route ?
  <cr>
  bgp             Border Gateway Protocol (BGP)
  connected       Connected
  isis            ISO IS-IS (ISIS)
  kernel          Kernel
  ospf            Open Shortest Path First (OSPF)
  rip             Routing Information Protocol (RIP)
```

[5] Si se utiliza la interfaz `null0`, la ruta se instala como inalcanzable.

```
static          Static routes
A.B.C.D         Network in the IP routing table to display
A.B.C.D/M       IP prefix <network>/<length>,  e.g.,  35.0.0.0/8
supernets-only  Show supernet entries only
```

Por ejemplo, se puede obtener información relativa a una red destino:

```
routerUC3M# show ip ro 192.168.2.3
Routing entry for 192.168.2.0/24
  Known via "connected", distance 0, metric 0, best
  * directly connected, eth0.2
```

- Para mostrar información sobre rutas IPv6, se utiliza la misma sintaxis, pero empleando "`show ipv6 route`" en vez de "`show ip route`".

3. CONFIGURACIÓN DE PROTOCOLOS DE ENCAMINAMIENTO

Esta sección incluye información acerca de la configuración de los protocolos de encaminamiento RIP, OSPF y BGP.

3.1 Configuración de RIP

A partir del modo de configuración del router (recuerde que para acceder a él, tiene que teclear `configure terminal` desde la consola inicial), se puede habilitar el protocolo de encaminamiento RIP, tecleando `router rip`. Para deshabilitarlo, debe teclear `no router rip`. Es necesario habilitar el protocolo RIP para poder acceder a los comandos de configuración del protocolo. El siguiente comando habilita el protocolo RIP en el router y proporciona acceso al sub-menú de configuración del protocolo RIP:

```
router(config)# router rip
router(config-router)#
```

Dentro del sub-menú de configuración del protocolo RIP, están disponibles los siguientes comandos:

Comandos de configuración básicos de RIP

- `network RED`
  - Este comando habilita el protocolo RIP en aquellos interfaces que posean direcciones IP pertenecientes a `RED`. Por ejemplo, si la red `10.0.0.0/24` está habilitada por RIP, esto significa que las direcciones desde `10.0.0.0` hasta `10.0.0.255` están habilitadas por RIP. El comando "`no network`" deshabilitará RIP de la red específica.
- `no network RED`
  - Deshabilita el protocolo RIP en las interfaces de red que posean direcciones IP pertenecientes a la red especificada.
- `network NOMBRE_DE_LA_INTERFAZ_DE_RED`
  - Este comando habilita el protocolo RIP en la interfaz de red `NOMBRE_DE_LA_INTERFAZ_DE_RED`. Se habilita tanto el envío como la recepción de paquetes RIP en la interfaz de red especificada.
- `no network NOMBRE_DE_LA_INTERFAZ_DE_RED`
  - Deshabilita el protocolo RIP en la interfaz de red especificada.
- `network neighbor A.B.C.D`
  - Especifica el nodo con dirección IP `A.B.C.D` como vecino RIP. Cuando un vecino no entiende multicast, este comando se utiliza para especificar los vecinos. En muchos casos, no todos los routers son capaces de entender multicast (los paquetes se envían a una dirección que especifica un grupo de receptores). En una situación donde el vecino no procesa los paquetes de multicast, es necesario establecer un enlace directo entre los routers. El comando `neighbor` permite al administrador de la red especificar un router como vecino de RIP.
- `no network neighbor A.B.C.D`
  - Deshabilita el nodo con dirección IP `A.B.C.D` como vecino RIP del router.
- `passive-interface NOMBRE_DE_LA_INTERFAZ_DE_RED`

  - Este comando configura el interfaz especificado (`NOMBRE_DE_LA_INTERFAZ_DE_RED`) en modo pasivo. Cuando un interfaz se configura en modo pasivo, todos los paquetes recibidos se procesan como normales y el router no envía paquetes RIP (ni multicast ni unicast) excepto a los vecinos especificados en el comando `neighbor`. Por defecto, todos los interfaces están configurados como pasivos
- `no passive-interface NOMBRE_DE_LA_INTERFAZ_DE_RED`
  - Configura el interfaz especificado (`NOMBRE_DE_LA_INTERFAZ_DE_RED`) como no pasivo.
- `version VERSIÓN`
  - Configura la versión del protocolo RIP para envío y recepción, la versión (`VERSIÓN`) puede ser "1" (RIPv1) o "2" (RIPv2). La versión por defecto es “2”.

Comandos de configuración de redistribución de rutas en RIP

- `redistribute kernel`
  - Habilita la redistribución de las rutas del *kernel* (aquellas que han sido creadas por un proceso interno del Sistema Operativo del router) en la tabla de RIP (ésta es la tabla que maneja internamente el protocolo de encaminamiento RIP, es decir la que incluye en los Vectores-Distancia que envía y la que actualiza con los mensajes RIP recibidos).
- `redistribute kernel metric <0-16>`
  - Igual que el anterior. pero especificando el valor de la métrica que se utiliza para anunciar estas rutas.
- `no redistribute kernel`
  - Deshabilita la redistribución de rutas del *kernel* en la tabla de RIP.
- `redistribute static`
  - Habilita la redistribución de las rutas estáticas en la tabla de RIP.
- `redistribute static metric <0-16>`
  - Igual que el anterior, pero especificando el valor de la métrica que se utiliza para anunciar estas rutas.
- `no redistribute static`
  - Deshabilita la redistribución de las rutas estáticas en la tabla de RIP.
- `redistribute connected`
  - Habilita la redistribución de las rutas directamente conectadas de aquellas interfaces con RIP deshabilitado en la tabla de RIP. Las rutas directamente conectadas de las interfaces con RIP habilitado está activada por defecto.
- `redistribute connected metric <0-16>`
  - Igual que el anterior, pero especificando el valor de la métrica que se utiliza para anunciar estas rutas.
- `no redistribute connected`
  - Deshabilita la redistribución de las rutas directamente conectadas en la tabla de RIP.
- `redistribute ospf`
  - Habilita la redistribución de las rutas aprendidas mediante el protocolo de encaminamiento OSPF en la tabla de RIP.
- `redistribute ospf metric <0-16>`
  - Igual que el anterior, pero especificando el valor de la métrica que se utiliza para anunciar estas rutas.
- `no redistribute ospf`
  - Deshabilita la redistribución de las rutas aprendidas mediante OSPF en la tabla de RIP.
- `redistribute bgp`
  - Habilita la redistribución de las rutas aprendidas mediante el protocolo de encaminamiento BGP en la tabla de RIP.
- `redistribute bgp metric <0-16>`
  - Igual que el anterior, pero especificando el valor de la métrica que se utiliza para anunciar estas rutas.
- `no redistribute bgp`
  - Deshabilita la redistribución de las rutas aprendidas mediante BGP en la tabla de RIP.
- `default-metric MÉTRICA`
  - Este comando modifica la métrica por defecto (`MÉTRICA`, entre 1 y 16) para las rutas distribuidas. El valor por defecto es 1. Este comando no afecta a la métrica de las rutas directamente conectadas directamente incluso si están redistribuidas mediante el comando `redistribute connected`. Para modificar el valor de la métrica de una ruta directamente conectada, es necesario utilizar el comando `redistribute conected metric.`

- `distance DISTANCIA`
  - Configura a un valor específico (`DISTANCIA`, entre 1 y 255) el valor de la distancia administrativa utilizada por el router para aquellas rutas aprendidas mediante RIP. Por defecto, la distancia administrativa de RIP es 120.
- `no distance DISTANCIA`
  - Restaura el valor por defecto de la distancia administrativa de RIP.
- `distance DISTANCIA A.B.C.D/M`
  - Configura a un valor específico (`DISTANCIA`, entre 1 y 255) el valor de la distancia administrativa RIP para aquellas rutas aprendidas por RIP dentro del rango `A.B.C.D/M`.
- `no distance DISTANCIA A.B.C.D/M`
  - Restaura el valor por defecto de la distancia administrativa RIP para aquellas rutas aprendidas por RIP dentro del rango `A.B.C.D/M`.
- `timers basic update timeout garbage`
  - Configura el valor de los temporizadores empleados por RIP: `update timeout garbage`. El valor por defecto de dichos temporizadores es el especificado por el estándar, es decir:
    - `update`. Valor por defecto: 30 segundos. Cada vez que el temporizador llega a 30 segundos se produce una actualización, el proceso de RIP despierta y envía un mensaje de respuesta no solicitado conteniendo la tabla completa de encaminamiento de todos los routers vecinos.
    - `timeout`. Valor por defecto: 180 segundos. Una vez llegado este tiempo sin haber recibido actualizaciones la ruta se considera no válida, sin embargo la ruta se retiene un cierto periodo de tiempo, lo cual permite avisar a los vecinos que la ruta ha sido eliminada.
    - `garbage`. Valor por defecto: 120 segundos. Una vez transcurrido este tiempo después de marcarse una ruta como no válida, la ruta es definitivamente eliminada de la tabla de encaminamiento.
- `no timers basic`
  - Resetea el valor de los temporizadores a sus valores por defecto (30, 180, 120).

Además de los comandos de configuración accesibles desde el sub-menú de configuración del protocolo RIP, algunos parámetros son configurables desde el sub-menú de configuración de interfaz (recuerde que puede acceder al sub-menú de configuración de una interfaz dada, tecleando `interface NOMBRE_DE_LA_INTERFAZ_DE_RED` desde el modo de configuración):

- `ip rip send version VERSIÓN`
  - Este comando de configuración sobrescribe (es decir, tiene preferencia sobre) el valor global establecido por el comando de configuración del protocolo RIP "`rip version`". Este comando habilita la interfaz de red seleccionada para enviar paquetes con versión RIP versión 1, RIP versión 2 o ambos. El parámetro `VERSIÓN` puede ser "1", "2" o "1 2". En el caso de elegir "1 2", los paquetes son enviados mediante broadcast y multicast. Por defecto, los paquetes enviados son RIPv2.
- `ip rip receive version VERSIÓN`
  - Este comando de configuración sobrescribe (es decir, tiene preferencia sobre) el valor global establecido por el comando de configuración del protocolo RIP "`rip version`". Este comando habilita en la interfaz de red seleccionada la recepción de paquetes RIP versión 1, RIP versión 2 o ambos. El parámetro `VERSIÓN` puede ser "1", "2" o "1 2". En el caso de elegir "1 2", acepta paquetes de ambas versiones (RIPv1 y RIPv2). Por defecto, se aceptan paquetes de ambas versiones de RIP.
- `ip split-horizon`
  - Habilita *split-horizon* en la interfaz de red seleccionada. Por defecto, *split-horizon* está activado.
- `no ip split-horizon`
  - Deshabilita *split-horizon* en la interfaz de red seleccionada.
- `ip split-horizon poisoned-reverse`
  - Habilita *split-horizon with poisoned-reverse* en la interfaz de red seleccionada.
- `no ip split-horizon poisoned-reverse`
  - Deshabilita *split-horizon with poisoned-reverse* en la interfaz de red seleccionada.
- `ip rip authentication mode md5`
  - Configura la interfaz de red seleccionada para utilizar autenticación de tipo MD5. Nota: si se activa algún tipo de autenticación en el router, el router seguirá contestando a paquetes de

tipo RIPv1 *REQUEST* (si la recepción de paquetes RIPv1 está activada), pero sólo los mensajes RIPv2 autenticados apropiadamente podrán actualizar la tabla de encaminamiento RIP del router.

- `no ip rip authentication mode md5`
  - Deshabilita la utilización de autenticación de tipo MD5 en la interfaz de red seleccionada.
- `ip rip authentication mode text`
  - Configura la interfaz de red seleccionada para utilizar autenticación de tipo "texto plano", utilizando una contraseña (enviada en texto plano) simple.
- `no ip rip authentication mode text`
  - Deshabilita la utilización de autenticación de tipo " texto plano" en la interfaz de red seleccionada.
- `ip rip authentication string CONTRASEÑA`
  - Configura contraseña a utilizar (`CONTRASEÑA`) cuando se emplea el mecanismo de autenticación RIP de tipo "texto plano". La longitud del texto `CONTRASEÑA` tiene que ser menor de 16 caracteres.
- `no ip rip authentication string CONTRASEÑA`
  - Borra la contraseña a utilizar (`CONTRASEÑA`) cuando se emplea el mecanismo de autenticación RIP de tipo "texto plano".
- `ip rip authentication key-chain CADENA_MD5`
  - Configura la cadena MD5 a utilizar (`CADENA_MD5`) cuando se emplea el mecanismo de autenticación RIP de tipo MD5.
- `no ip rip authentication key-chain CADENA_MD5`
  - Borra la contraseña a utilizar (`CADENA_MD5`) cuando se emplea el mecanismo de autenticación RIP de tipo MD5.

El modo terminal (el modo inicial de la consola del router, identificado con el *prompt* "`routerUC3M#`"), permite obtener información sobre el funcionamiento y estado del protocolo RIP (además de la información que se obtiene al consultar la tabla de encaminamiento global del router). Especialmente, son interesantes los siguientes comandos:

- `show ip rip`
  - Muestra las rutas RIP (las que contiene la tabla de encaminamiento RIP). Para rutas que han sido recibidas a través de RIP, este comando mostrará el tiempo que el paquete se envió y la información de la etiqueta. Este comando también mostrará esta información para las rutas redistribuidas por RIP. Por ejemplo:

```
routerUC3M# show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

     Network          Next Hop        Metric From           Tag Time
C(i) 10.0.0.0/24      0.0.0.0              1 self             0
R(n) 10.0.2.0/26      10.0.2.174           3 10.0.2.174       0 02:45
R(n) 10.0.2.64/26     10.0.2.174           3 10.0.2.174       0 02:45
R(n) 10.0.2.128/27    10.0.2.174           2 10.0.2.174       0 02:45
R(n) 10.0.2.160/30    10.0.2.174           3 10.0.2.174       0 02:45
R(n) 10.0.2.164/30    10.0.2.174           2 10.0.2.174       0 02:45
R(n) 10.0.2.168/30    10.0.2.174           2 10.0.2.174       0 02:45
C(i) 10.0.2.172/30    0.0.0.0              1 self
0
```

- show ip rip status
  - El comando muestra el estado actual de RIP. Esto incluye los temporizadores de RIP, versión, interfaces de red habilitadas y la información de los vecinos de RIP. Por ejemplo:

```
routerUC3M# show ip rip status
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 9 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive any version
    Interface        Send  Recv   Key-chain
    eth0.2            2     1 2
  Routing for Networks:
    eth0.2
```

```
Routing Information Sources:
  Gateway          BadPackets BadRoutes  Distance Last Update
Distance: (default is 120)
```

3.2 Configuración de OSPF

A partir del modo de configuración del router (recuerde que para acceder a él, tiene que teclear `configure terminal` desde la consola inicial), se puede habilitar el protocolo de encaminamiento RIP, tecleando `router ospf`. Para deshabilitarlo, debe teclear `no router ospf`. Es necesario habilitar el protocolo OSPF para poder acceder a los comandos de configuración del protocolo. El siguiente comando habilita el protocolo OSPF en el router y proporciona acceso al sub-menú de configuración del protocolo OSPF:

```
router(config)# router ospf
router(config-router)#
```

Dentro del sub-menú de configuración del protocolo OSPF, están disponibles los siguientes comandos:

Comandos de configuración básicos de OSPF

- `ospf router-id ROUTER-ID`
  - Este comando especifica el *router-ID* (identificador del router). Si no se especifica, por defecto se utiliza la dirección IP de mayor numeración de todos los interfaces como *router-ID*.
- `no ospf router-id ROUTER-ID`
  - Este comando restaura la configuración por defecto para el *router-ID* (la dirección IP de mayor numeración de todos los interfaces).
- `network RED area ÁREA`
  - Este comando habilita el protocolo OSPF en aquellos interfaces que posean direcciones IP pertenecientes a `RED`. Por ejemplo, si la red `10.0.0.0/24` está habilitada por OSPF, esto significa que las interfaces de red que tengan direcciones comprendidas desde `10.0.0.0` hasta `10.0.0.255` están habilitadas para OSPF. `ÁREA` puede tener el formato de una dirección IP o de un número entero entre 0 y 4294967295 (el router internamente hace la conversión a formato de dirección IP).
- `no network RED area ÁREA`
  - Deshabilita el protocolo OSPF en las interfaces de red que posean direcciones IP pertenecientes a la red especificada.
- `passive-interface NOMBRE_INTERFAZ`
  - Este comando configura el router para que no se "hable" OSPF en la interfaz `NOMBRE_INTERFAZ`, pero que sí que se anuncie la interfaz como un enlace de tipo *stub* en los mensajes LSA (*Link State Advertisement*) que envía el router. Esto permite al router anunciar las direcciones de interfaces directamente conectadas sin tener que generar LSAs de tipo 5 (*External*) que tienen un ámbito de inundación global, como ocurriría si se redistribuyeran las direcciones directamente conectadas en OSPF. Ésta es la única forma de anunciar enlaces en los que no se habla OSPF dentro de áreas de tipo *stub*.
- `no passive-interface NOMBRE_INTERFAZ`
  - Este comando deshace el comando anterior, habilitando que en la interfaz `NOMBRE_INTERFAZ` se "hable" OSPF si el router está configurado para anunciar direcciones configuradas en dicho interfaz.
- `ospf abr-type TIPO`
  - Este comando permite modificar el comportamiento estándar de un router OSPF de tipo ABR (*Access Border Router*). El protocolo estándar O*SPF no permite que un ABR considere rutas a través de áreas que no son de tipo* backbone cuando los enlaces del router hacia el *backbone* están caídas, incluso aunque existan otros ABRs conectados a áreas no *backbone* que sí que puedan alcanzar el *backbone.* Esta limitación existe principalmente para evitar que se formen bucles en el encaminamiento. `TIPO` puede ser `cisco`, `ibm`, `shortcut` o `standard`. Cuando se utiliza `cisco` o `ibm` (valor por defecto), la limitación anterior se relaja, permitiendo a un ABR considerar rutas aprendidas de otros ABRs a través de áreas no *backbone*, y por lo tanto encaminar a través de esas áreas no *backbone* como último recurso y sólo cuando los enlaces al *backbone* están caídos. Puede obtener más información sobre este comando en [1].

- `no ospf abr-type TIPO`
  - Restablece la configuración por defecto del tipo de comportamiento a utilizar por un router OSPF ABR.
- `timers spf VALOR_TIMER`
  - Este comando establece el retardo (*VALOR_TIMER*, expresado en milisegundos) que transcurre entre que ocurre un evento que hace que se tenga que recalcular la tabla de encaminamiento (en sentido estricto, el SPF) y el momento en que efectivamente se recalcula.
- `no timers spf`
  - Este comando establece el valor por defecto (1 segundo) al temporizador anterior.
- `auto-cost reference-bandwidth BW_REFERENCIA`
  - Este comando establece a `BW_REFERENCIA` el ancho de banda tomado como valor de referencia (aquél que tendría coste igual a 1) para el cálculo de los costes. `BW_REFERENCIA` se expresa en Mbit/s, siendo 100 Mbit/s el valor por defecto (es decir, enlaces con un ancho de banda de 100 Mbit/s o mayores tendrían un coste de 1). Este valor debe ser consistente en todos los routers de un dominio OSPF.

Comandos de configuración relativos a áreas OSPF

- `area ÁREA range PREFIJO/LONGITUD_PREFIJO`
  - Este comando agrega/resume rutas intra-área (del área especificada: ÁREA) que pertenezcan al rango `PREFIJO/LONGITUD_PREFIJO` en un sólo LSA de Tipo 3 (*Type-3, Network Summary LSA*) anunciado a otras áreas. Este comando sólo puede ser utilizado en un router de tipo ABR (*Access Border Router*) y sólo se pueden agregar/resumir LSAs de tipo 1 (*Type 1, Router-LSA*) o de tipo 2 (*Type 2, Network-LSA*).
- `no area ÁREA range PREFIJO/LONGITUD_PREFIJO`
  - Deshace la agregación anterior.
- `area ÁREA range PREFIJO/LONGITUD_PREFIJO not-advertise`
  - En vez de agregar/resumir rutas intra-área como hacía el comando anteriormente descrito, este comando filtra las rutas intra-área (del área especificada: ÁREA) que pertenezcan al rango `PREFIJO/LONGITUD_PREFIJO`, de forma que no son anunciadas a otras áreas. Este comando sólo tiene sentido en routers de tipo ABR (*Access Border Router*).
- `no area ÁREA range PREFIJO/LONGITUD_PREFIJO not-advertise`
  - Deshace la acción del comando anterior, permitiendo el anuncio de rutas pertenecientes al rango `PREFIJO/LONGITUD_PREFIJO` en `otras áreas.`
- `area ÁREA range PREFIJO/LONGITUD_PREFIJO substitute PREFIJO_SUST/LONGITUD_PREFIJO_SUST`
  - Este comando sustituye el prefijo agregado/resumido con otro prefijo. Este comando es análogo a "`area ÁREA range PREFIJO/LONGITUD_PREFIJO`" , pero en lugar de anunciar el prefijo agregado `PREFIJO/LONGITUD_PREFIJO`, lo sustituye por `PREFIJO_SUST/LONGITUD_PREFIJO_SUST` en los LSAs de tipo 3 generados. Este comando sólo tiene sentido en routers de tipo ABR.
- `no area ÁREA range PREFIJO/LONGITUD_PREFIJO substitute PREFIJO_SUST/LONGITUD_PREFIJO_SUST`
  - Deshace la acción del comando anterior, evitando que se generen LSAs de tipo 3 en los que se anuncia el prefijo sustituto.
- `area ÁREA stub`
  - Este comando configura el área como tipo *stub*, es decir, un área en la que ningún router origina rutas externas al dominio OSPF, y por lo tanto un área en el que todas las rutas al exterior son a través de routers de tipo ABR.
- `no area ÁREA stub`
  - Este comando deshace la configuración anterior, deshabilitando la configuración del área como tipo *stub*.
- `area ÁREA_STUB stub no-summary`
  - Este comando configura un router de tipo ABR para que no inyecte LSAs de tipo 3 (*Type 3, Network Summary*) en el área stub especificada (`ÁREA_STUB`).
- `no area ÁREA_STUB stub no-summary`
  - Este comando deshace la configuración anterior.
- `area ÁREA nssa`
  - Este comando configura el área como tipo *nssa.* De forma similar al caso de la configuración como *stub,* este comando admite diferentes parámetros adicionales referentes a aspectos particulares de la configuración áreas *nssa.*
- `no area ÁREA nssa`

- Este comando deshace la configuración anterior, deshabilitando la configuración del área como tipo *nssa*.

- `area ÁREA default-cost COSTE`
  - Este comando el coste por defecto (`COSTE`) de los LSAs anunciados (originados en el área `ÁREA`) a áreas de tipo *stub*.
- `no area ÁREA default-cost COSTE`
  - Este comando deshace la configuración anterior.
- `area ÁREA export-list NOMBRE_LISTA`
  - Este comando filtra los LSAs de tipo 3 (de rutas dentro del área `ÁREA`) a anunciar a otras áreas, aplicando la lista de tipo *access-list* de nombre `NOMBRE_LISTA`. Este comando sólo tiene sentido si el router actúa como router ABR del área especificada.
- `no area ÁREA export-list NOMBRE_LISTA`
  - Este comando deshace la configuración anterior, eliminando el filtro a través de la lista de tipo *access-list* `NOMBRE_LISTA` de las rutas (originadas dentro del área `ÁREA`) anunciadas a otras áreas.
- `area ÁREA import-list NOMBRE_LISTA`
  - Este comando es análogo al comando `area ÁREA export-list NOMBRE_LISTA`, pero filtrando las rutas a anunciar como LSAs de tipo 3 dentro del área ÁREA.
- `no area ÁREA import-list NOMBRE_LISTA`
  - Este comando deshace la configuración anterior, eliminando el filtro de las rutas a anunciar dentro del área `ÁREA`.
- `area ÁREA filter-list prefix NOMBRE_LISTA out`
  - Este comando filtra los LSAs de tipo 3 (de rutas dentro del área `ÁREA`) a anunciar a otras áreas, aplicando la lista de tipo *prefix-list* de nombre `NOMBRE_LISTA`. Este comando sólo tiene sentido si el router actúa como router ABR del área especificada.
- `no area ÁREA filter-list prefix NOMBRE_LISTA out`
  - Este comando deshace la configuración anterior, eliminando el filtro a través de la lista de tipo *prefix-list* `NOMBRE_LISTA` de las rutas (originadas dentro del área `ÁREA`) anunciadas a otras áreas.
- `area ÁREA filter-list prefix NOMBRE_LISTA in`
  - Este comando filtra los LSAs de tipo 3 a anunciar dentro del área `ÁREA` , aplicando la lista de tipo *prefix-list* de nombre `NOMBRE_LISTA`. Este comando sólo tiene sentido si el router actúa como router ABR del área especificada.
- `no area ÁREA filter-list prefix NOMBRE_LISTA in`
  - Este comando deshace la configuración anterior, eliminando el filtro a través de la lista de tipo *prefix-list* `NOMBRE_LISTA` de las rutas a anunciar dentro del área `ÁREA`.
- `area ÁREA authentication`
  - Este comando especifica que se debe utilizar autenticación simple basada en contraseña en el área `ÁREA`.
- `no area ÁREA authentication`
  - Este comando desactiva la autenticación por contraseña en el área `ÁREA`.
- `area ÁREA authentication message-digest`
  - Este comando especifica que se debe utilizar autenticación de tipo MD5-HMAC en el área `ÁREA`. El material criptográfico se proporciona utilizando comandos OSPF dentro del sub-menú de interfaz.
- `no area ÁREA authentication message-digest`
  - Este comando desactiva la autenticación de tipo MD5-HMAC en el área `ÁREA`.

<u>Comandos de configuración de redistribución de rutas de OSPF</u>

- `redistribute kernel`
  - Este comando habilita la redistribución de las rutas del *kernel* (aquellas que han sido creadas por un proceso interno del Sistema Operativo del router) en OSPF.
- `no redistribute kernel`
  - Este comando deshabilita la redistribución de las rutas del *kernel* en OSPF.
- `redistribute connected`
  - Este comando habilita la redistribución de las rutas directamente conectadas en OSPF. Esto puede hacerse también utilizando el comando "`passive-interface NOMBRE_INTERFAZ`".
- `no redistribute connected`
  - Este comando deshabilita la redistribución de las rutas directamente conectadas en OSPF.
- `redistribute static`

  - Este comando habilita la redistribución de las rutas estáticas en OSPF.
- `no redistribute static`
  - Este comando deshabilita la redistribución de las rutas estáticas en OSPF.
- `redistribute rip`
  - Este comando habilita la redistribución de las rutas aprendidas mediante el protocolo de encaminamiento RIP en OSPF.
- `no redistribute rip`
  - Este comando deshabilita la redistribución de las rutas aprendidas mediante el protocolo de encaminamiento RIP en OSPF.
- `redistribute bgp`
  - Este comando habilita la redistribución de las rutas aprendidas mediante el protocolo de encaminamiento BGP en OSPF.
- `no redistribute bgp`
  - Este comando deshabilita la redistribución de las rutas aprendidas mediante el protocolo de encaminamiento BGP en OSPF.
- `redistribute (kernel|connected|static|rip|bgp) metric MÉTRICA route-map MAPA`
  - A cualquiera de los comandos de redistribución de rutas anteriores se les puede añadir información acerca de la métrica (`MÉTRICA`) a utilizar en OSPF con las rutas redistribuidas, y/o aplicar un filtro sobre las rutas a redistribuir, utilizando el *route-map* de nombre `MAPA`.
- `default-information originate [always]`
  - Este habilita que el router anuncia una ruta por defecto mediante LSAs de tipo 5 (*Type 5, AS-External*) en todas las áreas que soporten rutas externas a OSPF. Si el parámetro `always` está presente, la ruta por defecto se anuncia aunque no esté presente en la tabla de rutas del router. Al igual que el comando "`redistribute`", también puede recibir parámetros opcionales para establecer la métrica con la que se anuncia esta ruta o para realizar un filtrado de la misma aplicando un *route-map*.
- `no default-information originate`
  - Este comando deshabilita el anuncio de una ruta por defecto en LSAs de tipo 5.
- `distribute-list NOMBRE_LISTA out (kernel|connected|static|rip)`
  - Este comando aplica la lista de tipo *access-list* (de nombre `NOMBRE_LISTA`) a las rutas a redistribuir del tipo especificado (`kernel|connected|static|rip`).
- `no distribute-list NOMBRE_LISTA out (kernel|connected|static|rip)`
  - Este comando deshabilita el filtrado anterior sobre las rutas a redistribuir.
- `distance DISTANCIA`
  - Configura a un valor específico (`DISTANCIA`, entre 1 y 255) el valor de la distancia administrativa utilizada por el router para aquellas rutas aprendidas mediante OSPF. Por defecto, la distancia administrativa de OSPF es 110.
- `no distance DISTANCIA`
  - Restaura el valor por defecto de la distancia administrativa de OSPF.
- `distance ospf (intra-area|inter-area|external) DISTANCIA`
  - Configura a un valor específico (`DISTANCIA`, entre 1 y 255) el valor de la distancia administrativa utilizada por el router para aquellas rutas aprendidas mediante OSPF dentro del mismo área (`intra-area`), de un área diferente (`inter-area`) o mediante una ruta externa a OSPF (`external`). Por defecto, la distancia administrativa de OSPF es 110.
- `no distance ospf`
  - Restaura el valor por defecto de las distancias administrativas (`intra-area|inter-area|external`) de OSPF.
- `default-metric MÉTRICA`
  - Este comando establece el valor por defecto de la métrica (`MÉTRICA`) a utilizar en OSPF.
- `no default-metric`
  - Este comando restaura el valor por defecto de la métrica a utilizar en OSPF.

Además de los comandos de configuración accesibles desde el sub-menú de configuración del protocolo OSPF, algunos parámetros son configurables desde el sub-menú de configuración de interfaz (recuerde que puede acceder al sub-menú de configuración de una interfaz dada, tecleando `interface NOMBRE_DE_LA_INTERFAZ_DE_RED` desde el modo de configuración):

- `ip ospf authentication-key CLAVE`

- Este comando establece la clave a utilizar como contraseña simple. La contraseña `CLAVE` debe tener 8 caracteres de longitud como máximo.

- `no ip ospf authentication-key`
  - Este comando borra la clave a utilizar como contraseña simple.
- `ip ospf authentication message-digest`
  - Este comando especifica que se debe utilizar autenticación de tipo MD5-HMAC en este interfaz. Este comando sobrescribe (es decir, tiene preferencia sobre) el valor global establecido por el comando de configuración del protocolo OSPF "`area ÁREA authentication message-digest`".
- `ip ospf authentication message-digest-key ID_CLAVE key CLAVE`
  - Este comando especifica la clave a utilizar. `ID_CLAVE` identifica la clave secreta utilizada para crear la firma del mensaje. Este identificador es parte del protocolo y debe ser consistente en todos los routers en un enlace. `CLAVE` es la clave propiamente dicha, con una longitud máxima de 16 caracteres (las claves más largas se truncan) y asociada al identificador de clave `ID_CLAVE`.
- `no ip ospf authentication message-digest-key`
  - Este comando borra la clave a utilizar.
- `ip ospf cost COSTE`
  - Este comando establece el coste (`COSTE`, entre 1 y 65535) de la interfaz.
- `no ip ospf cost`
  - Este comando borra el valor del coste de la interfaz configurado anteriormente.
- `ip ospf dead-interval INTERVALO`
  - Este comando establece el valor (`INTERVALO`, entre 1 y 65535) del temporizador *RouterDeadInterval* usado para los temporizadores *Wait Timer* e *Inactivity Interval*. Este valor debe ser el mismo para todos los routers conectados a una misma red. El valor por defecto es 40 segundos. Puede encontrar más información en [1].
- `no ip ospf dead-interval`
  - Este comando restablece el valor por defecto del temporizador.
- `ip ospf hello-interval INTERVALO`
  - Este comando establece el valor del intervalo de tiempo (`INTERVALO`, entre 1 y 65535) en segundos entre envíos de mensajes *HELLO* en el interfaz. El valor por defecto es 10 segundos.
- `no ip ospf hello-interval`
  - Este comando restablece el valor por defecto del temporizador de envío de mensajes *HELLO*.
- `ip ospf network (broadcast|non-broadcast|point-to-multipoint|point-to-point)`
  - Este comando establece el tipo de red al que pertenece la interfaz.
- `no ip ospf network`
  - Este comando deshace la configuración del comando anterior.
- `ip ospf priority PRIORIDAD`
  - Este comando establece el valor de la prioridad (`PRIORIDAD`, entre 0 y 255) del router (*RouterPriority*). Cuanto más alto sea este valor, más probable es que resulte elegido como router designado. Un valor de `PRIORIDAD` igual a 0 hace que sea imposible que sea elegido como router designado. El valor por defecto es 1.
- `no ip ospf priority`
  - Este comando restablece el parámetro prioridad del router (*RouterPriority*) a su valor por defecto.
- `ip ospf retransmit-interval INTERVALO`
  - Este comando establece el valor del intervalo (`INTERVALO`, entre 1 y 65535) entre retransmisiones de los mensajes de tipo *Database Description* y *Link State Request*. El valor por defecto es 5 seundos.
- `no ip ospf retransmit-interval`
  - Este comando restablece el valor del intervalo de retransmisión anterior a su valor por defecto.

El modo terminal (el modo inicial de la consola del router, identificado con el *prompt* "`routerUC3M#`"), permite obtener información sobre el funcionamiento y estado del protocolo OSPF (además de la información que se obtiene al consultar la tabla de encaminamiento global del router). Especialmente, son interesantes los siguientes comandos:

- `show ip ospf`
  - Muestra información general sobre la configuración de OSPF y el estado de las áreas.
- `show ip ospf interface NOMBRE_INTERFAZ`
  - Muestra información general sobre la configuración OSPF en el interfaz `NOMBRE-INTERFAZ`. Si no se especifica una interfaz, se muestra la información para todas las interfaces.

3.3 Configuración de BGP

A partir del modo de configuración del router (recuerde que para acceder a él, tiene que teclear `configure terminal` desde la consola inicial), se puede habilitar el protocolo de encaminamiento BGP, con el comando `router bgp NÚMERO_AS`. Para deshabilitarlo, debe teclear `no router bgp NÚMERO_AS`. Es necesario habilitar el protocolo BGP para poder acceder a los comandos de configuración del protocolo. El número de Sistema Autónomo (*Autonomous System*, AS) es utilizado por el router para detectar si una conexión es iBGP o eBGP. El número de AS es un número entero entre 1 y 65535. Los números de AS del 64512 al 65535 se definen como números de uso privado. Los número sde AS privados no deben nunca anunciarse a la Internet global pública.

El siguiente comando habilita el protocolo BGP en el router – utilizando 65001 como número de Sistema Autónomo – y proporciona acceso al sub-menú de configuración del protocolo BGP:

```
router(config)# router bgp 65001
router(config-router)#
```

Dentro del sub-menú de configuración del protocolo BGP, están disponibles los siguientes comandos:

<u>Comandos de configuración básicos de BGP</u>

- `bgp router-id ROUTER-ID`
  - Este comando especifica el *router-ID* (identificador del router). Si no se especifica, por defecto se utiliza la dirección IP de mayor numeración de todos los interfaces como *router-ID*.
- `no bgp router-id ROUTER-ID`
  - Este comando restaura la configuración por defecto para el *router-ID* (la dirección IP de mayor numeración de todos los interfaces).

<u>Comandos de configuración de anuncios de rutas BGP</u>

- `network RED`
  - Este comando activa el anuncio de una ruta a `RED` por BGP. Es muy recomendable que exista una ruta en el router hacia `RED` para anunciarla por BGP, puesto que muchos fabricantes de routers no envían anuncios BGP hacia aquellos destinos que no están presentes en la tabla de rutas local.
- `no network RED`
  - Desactiva el anuncio por BGP de la ruta hacia el destino `RED`.
- `redistribute kernel`
  - Habilita la redistribución de las rutas del *kernel* (aquellas que han sido creadas por un proceso interno del Sistema Operativo del router) en BGP.
- `no redistribute kernel`
  - Deshabilita la redistribución de rutas del *kernel* en BGP.
- `redistribute static`
  - Habilita la redistribución de las rutas estáticas en BGP.
- `no redistribute static`
  - Deshabilita la redistribución de las rutas estáticas en BGP.
- `redistribute connected`
  - Habilita la redistribución de las rutas directamente conectadas en BGP.
- `no redistribute connected`
  - Deshabilita la redistribución de las rutas directamente conectadas en BGP.
- `redistribute rip`
  - Habilita la redistribución de las rutas aprendidas mediante el protocolo de encaminamiento RIP en BGP.

- `no redistribute rip`
  - Deshabilita la redistribución de las rutas aprendidas mediante RIP en BGP.
- `redistribute ospf`
  - Habilita la redistribución de las rutas aprendidas mediante el protocolo de encaminamiento OSPF en BGP.
- `no redistribute ospf`
  - Deshabilita la redistribución de las rutas aprendidas mediante OSPF en BGP.

Comandos de configuración de vecinos BGP

- `neighbor DIR_IP_VECINO remote-as NÚMERO-AS`
  - Crea un nuevo vecino (cuya dirección IP es `DIR_IP_VECINO`) cuyo número de AS es `NÚMERO-AS`. Este es el primer comando que se debe introducir cuando se configura un vecino, en caso contrario se produciría un error.
- `no neighbor DIR_IP_VECINO remote-as NÚMERO-AS`
  - Elimina el vecino – con dirección IP `DIR_IP_VECINO` perteneciente al AS de número `NÚMERO-AS` – y toda la configuración asociada a él.
- `neighbor DIR_IP_VECINO shutdown`
  - Desactiva el vecino – cuya dirección IP `DIR_IP_VECINO` – manteniendo la configuración asociada a este. Este comando se utiliza cuando se quiere tirar la sesión con un vecino pero preservando toda su configuración. Se puede desactivar un vecino con el comando `"no neighbor DIR_IP_VECINO remote-as NÚMERO-AS"` pero a la vez borraríamos la configuración asociada.
- `no neighbor DIR_IP_VECINO shutdown`
  - Este comando activa de nuevo la sesión con el vecino cuya dirección IP es `DIR_IP_VECINO`.
- `neighbor DIR_IP_VECINO ebgp-multihop [TTL]`
  - Activa el modo *ebgp-multihop*, usado para establecer sesiones BGP entre sistemas de distintos AS que no se encuentran directamente conectados al mismo segmento de red y en ciertas configuraciones de túneles *GRE* e *IPIP*. El campo opcional `TTL` establece el número de saltos a los que se encuentra el vecino; si no se especifica, el valor por defecto es el máximo, 255.
- `no neighbor DIR_IP_VECINO ebgp-multihop`
  - Desactiva la configuración *ebgp-multihop*.
- `neighbor DIR_IP_VECINO description`
  - Añade una descripción textual (de longitud máxima 80 caracteres) de la sesión con un vecino (cuya dirección IP es `DIR_IP_VECINO`).
- `no neighbor DIR_IP_VECINO description`
  - Elimina la descripción textual de la sesión con un vecino (cuya dirección IP es `DIR_IP_VECINO`).
- `neighbor DIR_IP_VECINO version VERSIÓN`
  - Establece la versión del protocolo BGP del vecino (cuya dirección IP es `DIR_IP_VECINO`). `VERSIÓN` puede ser 4, 4+ o 4-. La versión 4 es el valor por defecto para las conexiones BGP. La versión 4+ significa que el vecino soporta extensiones Multiprotocolo para BGP.
- `no neighbor DIR_IP_VECINO version VERSIÓN`
  - Elimina la configuración anterior, restableciendo la versión por defecto (4)..
- `neighbor DIR_IP_VECINO next-hop-self`
  - Este comando fuerza a que el router se anuncie como siguiente salto en las rutas que distribuya al vecino con dirección IP `DIR_IP_VECINO`.
- `no neighbor DIR_IP_VECINO next-hop-self`
  - Deshace la configuración anterior, no forzando a que el router se anuncie como siguiente salto en las rutas que distribuya al vecino con dirección IP `DIR_IP_VECINO`.
- `neighbor DIR_IP_VECINO update-source DIR_IP`
  - Este comando especifica la dirección IP origen (`DIR_IP`) que se utilizará para establecer la sesión BGP con el vecino con dirección IP `DIR_IP_VECINO`.
- `no neighbor DIR_IP_VECINO update-source DIR_IP`
  - Deshace la configuración del comando anterior, no forzando la dirección IP origen que se utilizará al establecer la sesión con el vecino.
- `neighbor DIR_IP_VECINO update-source NOMBRE_INTERFAZ`

- Este comando especifica la dirección IP origen (se utiliza la dirección IP asignada a la interfaz `NOMBRE_INTERFAZ`) que se utilizará para establecer la sesión BGP con el vecino con dirección IP `DIR_IP_VECINO`.
- `no neighbor DIR_IP_VECINO update-source NOMBRE_INTERFAZ`
  - Deshace la configuración del comando anterior, no forzando la dirección IP origen que se utilizará al establecer la sesión con el vecino.
- `neighbor DIR_IP_VECINO default-originate`
  - El comportamiento por defecto del router es no anunciar mediante BGP la ruta por defecto (0.0.0.0/0), incluso aunque esté presente en la tabla de rutas. Este comando habilita el anuncio de la ruta por defecto al vecino de dirección IP `DIR_IP_VECINO`.
- `no neighbor DIR_IP_VECINO default-originate`
  - Deshabilita el anuncio de la ruta por defecto al vecino de dirección IP `DIR_IP_VECINO`.
- `neighbor DIR_IP_VECINO port PUERTO`
  - Especifica el puerto TCP que se usará para establecer la sesión BGP con el vecino de dirección IP `DIR_IP_VECINO`. Por defecto, se utiliza el puerto estándar (179).
- `no neighbor DIR_IP_VECINO port PUERTO`
  - Deshace el comando anterior, estableciendo el valor del puerto TCP por defecto (179) que se usará para establecer la sesión BGP con el vecino de dirección IP `DIR_IP_VECINO`.
- `neighbor DIR_IP_VECINO send-community`
  - Habilita el envío de las comunidades (*communities*) asociadas a los distintos prefijos anunciados. Este es el comportamiento por defecto.
- `no neighbor DIR_IP_VECINO send-community`
  - Deshabilita el envío de las comunidades (*communities*) asociadas a los distintos prefijos anunciados.
- `neighbor DIR_IP_VECINO weight PESO`
  - Especifica un peso por defecto a las rutas aprendidas del vecino especificado (cuya dirección IP es `DIR_IP_VECINO`. El atributo w*eight* es un atributo propietario de Cisco que se usa localmente en un router para elegir la mejor ruta cuando hay varias disponibles hacia un mismo destino. Este atributo no se transporta en ningún anuncio BGP (ni iBGP ni eBGP).
- `no neighbor DIR_IP_VECINO weight PESO`
  - Deshace el comando anterior.
- `neighbor DIR_IP_VECINO maximum-prefix NÚMERO_PREF`
  - Este comando fija un valor máximo en el número de prefijos (`NÚMERO_PREF`) que un vecino (cuya dirección IP es `DIR_IP_VECINO`) nos puede enviar. Se utiliza para evitar una inundación de prefijos que ponga en peligro la estabilidad de la red. Al llegar al número máximo de prefijos la sesión se cerrará hasta que el administrador, ejecute el comando "`no neighbor DIR_IP_VECINO shutdown`".
- `no neighbor DIR_IP_VECINO maximum-prefix NÚMERO_PREF`
  - Deshace el comando anterior, eliminando el número máximo de prefijos que un vecino nos puede enviar.

Comandos de configuración de filtrado de rutas a/de vecinos BGP[6]

- `neighbor DIR_IP_VECINO distribute-list NOMBRE_LISTA [IN | OUT]`
  - Este comando activa el uso de una lista de tipo *distribute-list* (aquella cuyo nombre es `NOMBRE_LISTA`) para el filtrado de anuncios BGP. Si se utiliza el parámetro `IN`, el filtrado es de los anuncios recibidos del vecino con dirección IP `DIR_IP_VECINO`, mientras que si el parámetro es `OUT`, el filtrado se realiza sobre los anuncios a enviar al vecino.
- `no neighbor DIR_IP_VECINO distribute-list NOMBRE_LISTA [IN | OUT]`
  - Deshace el comando anterior, eliminando el uso de la *distribute-list* para el filtrado de anuncios BGP a/desde un vecino.
- `neighbor DIR_IP_VECINO prefix-list NOMBRE_LISTA [IN | OUT]`
  - Este comando activa el uso de una lista de tipo *prefix-list* (aquella cuyo nombre es `NOMBRE_LISTA`) para el filtrado de anuncios BGP. Si se utiliza el parámetro `IN`, el

[6] Cada vez que realice cambios relativos a políticas de filtrado de rutas recibidas/enviadas a vecinos BGP, debe reiniciar las actualizaciones de información BGP con los vecinos afectados. Puede utilizar para ello, por ejemplo, el comando "`clear ip bgp *`" desde el modo terminal (el modo inicial de la consola del router, identificado con el *prompt* "`routerUC3M#`").

filtrado es de los anuncios recibidos del vecino con dirección IP `DIR_IP_VECINO`, mientras que si el parámetro es `OUT`, el filtrado se realiza sobre los anuncios a enviar al vecino.

- `no neighbor DIR_IP_VECINO prefix-list NOMBRE_LISTA [IN | OUT]`
  - Deshace el comando anterior, eliminando el uso de la *prefix-list* para el filtrado de anuncios BGP a/desde un vecino.
- `neighbor DIR_IP_VECINO filter-list NOMBRE_LISTA [IN | OUT]`
  - Este comando activa el uso de una lista de tipo *filter-list* (aquella cuyo nombre es `NOMBRE_LISTA`) para el filtrado de anuncios BGP. Si se utiliza el parámetro `IN`, el filtrado es de los anuncios recibidos del vecino con dirección IP `DIR_IP_VECINO`, mientras que si el parámetro es `OUT`, el filtrado se realiza sobre los anuncios a enviar al vecino.
- `no neighbor DIR_IP_VECINO filter-list NOMBRE_LISTA [IN | OUT]`
  - Deshace el comando anterior, eliminando el uso de la *filter-list* para el filtrado de anuncios BGP a/desde un vecino.
- `neighbor DIR_IP_VECINO route-map NOMBRE_MAPA [IN | OUT]`
  - Este comando activa el uso de un *route-map* (de nombre `NOMBRE_MAPA`) para un filtrado avanzado de los anuncios BGP. Si se utiliza el parámetro `IN`, el filtrado es de los anuncios recibidos del vecino con dirección IP `DIR_IP_VECINO`, mientras que si el parámetro es `OUT`, el filtrado se realiza sobre los anuncios a enviar al vecino.
- `no neighbor DIR_IP_VECINO route-map NOMBRE_MAP [IN | OUT]`
  - Deshace el comando anterior, eliminando el uso del *route-map* para el filtrado avanzado de anuncios BGP a/desde un vecino.

Comandos de configuración de grupos de vecinos BGP

- `neighbor NOMBRE_GRUPO peer-group`
  - Este comando crea un nuevo grupo de vecinos (*peer-group*) BGP. Dado que es habitual que algunos routers tengan una lista de vecinos muy larga, es útil poder definir grupos de vecinos a los que se les aplique el mismo tipo de configuración (por ej., políticas de filtrado de rutas). Estos grupos de vecinos reciben el nombre de *peer-groups*.
- `neighbor DIR_IP_VECINO peer-group NOMBRE_GRUPO`
  - Este comando añade el vecino BGP cuya dirección IP es `DIR_IP_VECINO` al *peer-group* de nombre `NOMBRE_GRUPO`.

Comandos de configuración de distancias administrativas BGP

- `distance bgp DIST_EXTERNAS DIST_INTERNAS DIST_LOCALES`
  - Este comando cambia el valor de la distancia administrativa que se utiliza cuando se insertan en la tabla de encaminamiento las rutas aprendidas por BGP. `DIST_EXTERNAS` es el valor a utilizar para las rutas aprendidas por eBGP, `DIST_INTERNAS` es el valor a utilizar para las rutas aprendidas por iBGP y `DIST_LOCALES` es el valor a utilizar para las rutas locales. Estos parámetros pueden tomar valores entre 1 y 255 y los valores por defecto son 20, 200 y 200 para `DIST_EXTERNAS`, `DIST_INTERNAS` y `DIST_LOCALES` respectivamente.
- `no distance bgp`
  - Restaura los valores por defecto de las distancias administrativas a utilizar por las rutas aprendidas por BGP.

Comandos de configuración de agregación de rutas en BGP

- `aggregate-address A.B.C.D/M`
  - Este comando especifica que se cree una entrada agregada en la tabla BGP si existen rutas más específicas que pertenecen al rango especificado `A.B.C.D/M`. La ruta agregada será anunciada como si se originara en su Sistema Autónomo y tendrá el atributo *atomic aggregate* activado para mostrar que cierta información de encaminamiento puede no estar disponible.
- `aggregate-address A.B.C.D/M as-set`
  - Este comando especifica que se cree una entrada agregada en la tabla BGP si existen rutas más específicas que pertenecen al rango especificado `A.B.C.D/M` tal y como hace el comando "`aggregate-address A.B.C.D/M`" , pero el camino anunciado en esta ruta será un *AS_SET* consistente en todos los elementos contenidos en todos los caminos que están siendo resumidos.
- `aggregate-address A.B.C.D/M summary-only`

- Este comando especifica no sólo que se cree una entrada agregada en la tabla BGP si existen rutas más específicas que pertenecen al rango especificado `A.B.C.D/M` tal y como hace el comando "`aggregate-address A.B.C.D/M`" , sino que no se anuncien a ningún vecino las rutas más específicas que están siendo agregadas.

- `no aggregate-address A.B.C.D/M`
  - Deshace la agregación de rutas.

El modo terminal (el modo inicial de la consola del router, identificado con el *prompt* "`routerUC3M#`"), permite obtener información sobre el funcionamiento y estado del protocolo BGP (además de la información que se obtiene al consultar la tabla de encaminamiento global del router). Especialmente, son interesantes los siguientes comandos:

- `show ip bgp`
  - Muestra todas las rutas BGP (las que contiene la tabla de encaminamiento BGP) que tiene el router. Por ejemplo:

```
routerUC3M# show ip bgp
BGP table version is 0, local router ID is 192.168.100.100
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      192.168.100.1            0             0 65001 i
*                   192.168.150.2                          0 65200 65001 i
*> 192.168.1.0/26   192.168.100.1            0             0 65001 i
*> 192.168.1.64/26  192.168.150.2                          0 65200 65001 i
*  192.168.2.0      192.168.150.2                          0 65200 65002 i
*>                  192.168.100.2            0             0 65002 i
*> 192.168.2.0/26   192.168.100.2            0             0 65002 i
*> 192.168.2.64/26  192.168.150.2                          0 65200 65002 i

Total number of prefixes 6
```

- `show ip bgp DESTINO`
  - Muestra las rutas BGP (las que contiene la tabla de encaminamiento BGP) hacia `DESTINO` que tiene el router. Por ejemplo:

```
routerUC3M# sh ip bgp 192.168.1.0/26
BGP routing table entry for 192.168.1.0/26
Paths: (3 available, best #3, table Default-IP-Routing-Table)
  Not advertised to any peer
  65200 65100 65001
    192.168.200.200 from 192.168.200.200 (192.168.200.200)
      Origin IGP, localpref 110, valid, external
      Last update: Sat Jan  1 23:30:52 2000

  65100 65001
    192.168.100.100 from 192.168.100.100 (192.168.100.100)
      Origin IGP, localpref 100, valid, external
      Last update: Sat Jan  1 23:30:52 2000

  65001
    10.0.0.1 from 10.0.0.1 (192.168.100.1)
      Origin IGP, metric 0, localpref 120, valid, external, best
      Last update: Sat Jan  1 23:30:46 2000
```

- `show ip bgp summary`
  - Muestra los atributos generales de la tabla de BGP y el estado de los vecinos configurados. Por ejemplo:

```
routerUC3M# sh ip bgp summary
BGP router identifier 192.168.100.100, local AS number 65100
4 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.100.1   4 65001      24      91        0    0    0 00:00:42        2
192.168.100.2   4 65002      10      17        0    0    0 00:01:54        2
192.168.150.2   4 65200     153     158        0    0    0 02:24:19        4

Total number of neighbors 3
```

- `show ip bgp summary DIR_IP_VECINO`
  - Muestra información detallada del vecino con dirección IP `DIR_IP_VECINO` y sus parámetros de configuración.
- `clear ip bgp DIR_IP_VECINO`

- Reinicia la sesión BGP en frío (desde cero) con el vecino con dirección IP `DIR_IP_VECINO`.
- `clear ip bgp *`
  - Reinicia la sesión BGP en frío (desde cero) con todos los vecinos.
- `clear ip bgp DIR_IP_VECINO soft`
  - Reinicio suave (no se resetea la conexión TCP) de la sesión BGP con el vecino con dirección IP `DIR_IP_VECINO`.
- `clear ip bgp DIR_IP_VECINO * soft`
  - Reinicio suave (no se resetea la conexión TCP) de la sesión BGP con todos los vecinos.

3.4 Herramientas de control y filtrado administrativo de la información de routing

En multitud de circunstancias, el administrador de una red necesita de herramientas que le permitan realizar un control y filtrado sobre la información de encaminamiento que recibe/envía/redistribuye. Por ejemplo, si se ejecuta más de un protocolo de encaminamiento en una red, es interesante disponer de mecanismos que permitan controlar cómo se redistribuye la información obtenida por un protocolo de encaminamiento en la red utilizando otro protocolo de encaminamiento diferente. Otro ejemplo en el que se necesita de esta clase de herramientas es BGP, para implementar políticas de encaminamiento, filtrar información originada en ciertas redes, etc. Esta sección introduce brevemente algunas de las herramientas más utilizadas en la práctica, prestando más atención a aquellas que se van a utilizar en las prácticas.

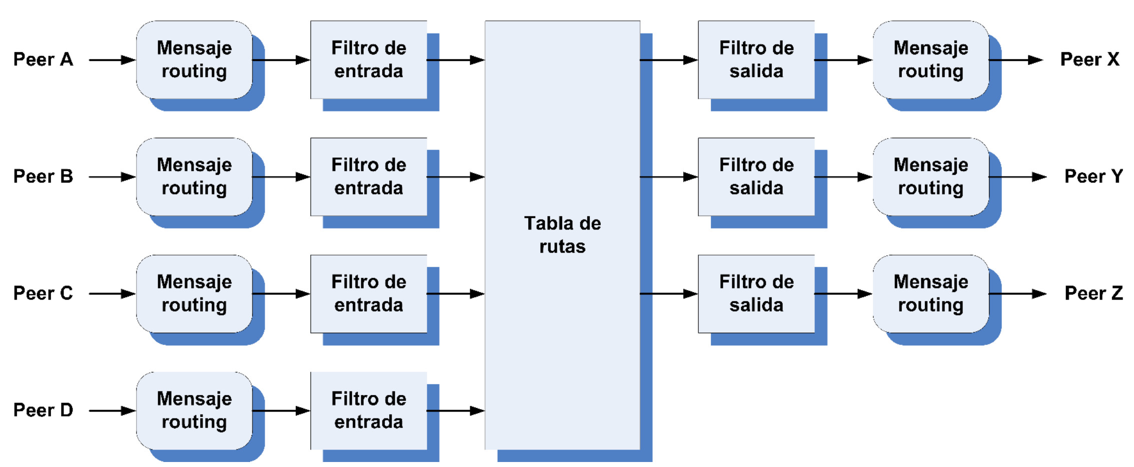


Figura 3: Filtrado de información de routing entrante y saliente

El esquema genérico que se utiliza para filtrar la información de encaminamiento en un router aparece en la Figura 3. Se pueden filtrar las rutas anunciadas por otro router (*peer*) con el que estamos intercambiando información de encaminamiento (utilizando un protocolo de routing) y evitar que éstas sean introducidas en la tabla de rutas de nuestro router. Para ello, podemos emplear filtros de entrada. Por otro lado, podemos filtrar las rutas que anunciamos a otros *peers*, utilizando para ello filtros de salida antes de enviar los mensajes de routing. A continuación, vamos a describir algunas herramientas que se pueden utilizar para implementar esta clase de filtros.

filter-lists

Las listas de tipo *filter-list* utilizan expresiones regulares simplificadas para implementar filtros de caminos BGP (AS-PATH). Debido a esto, este tipo de listas sólo pueden utilizarse trabajando con el protocolo BGP. Típicamente, este tipo de listas se utiliza para filtrar todas las rutas que tienen una longitud mayor que un cierto umbral. Las expresiones regulares de AS-PATH están basadas en las expresiones regulares POSIX. Los routers Cisco disponen de una implementación bastante limitada de expresiones regulares, por lo que es complicado implementar filtros complejos. Puede encontrar más información en [2].

distribute-lists

Las listas de tipo *distribute-list* son listas de acceso regulares que permiten filtrar direcciones IP. Este tipo de listas pueden utilizarse por todos los protocolos de encaminamiento.

Las listas de acceso (*access control lists*, ACL) son un método genérico de hacer búsqueda de patrones basada en información de protocolo. Principalmente, las listas de acceso se utilizan para restringir el acceso por razones de seguridad o para filtrar información de encaminamiento.
Existen varios tipos de listas de acceso. Las listas de acceso de tipo *standard* están numeradas de 1 a 99 o de 1300 a 1999 y sólo pueden buscar la coincidencia de la dirección origen para filtrar paquetes o la dirección de red destino para filtrar rutas. Este tipo de listas son útiles para filtrar rutas sin tener en cuenta la longitud del prefijo, por ejemplo (este ejemplo aparece en [3]) para filtrar las direcciones IP privadas:

```
router(config)# router bgp 60055
router(config-router)# neighbor 192.0.254.17 distribute-list 10 in
router(config-router)# exit
router(config)# access-list 10 deny 10.0.0.0 0.255.255.255
router(config)# access-list 10 deny 172.16.0.0 0.15.255.255
router(config)# access-list 10 deny 192.168.0.0 0.0.255.255
router(config)# access-list 10 permit any
router(config)# exit
```

Una lista de acceso está formada por una o varias entradas ordenadas, que se van recorriendo en búsqueda de una coincidencia. Cada entrada está configurada para permitir (*permit*) o denegar (*deny*) en caso de coincidencia. El router deja de procesar la lista de acceso cuando encuentra una entrada coincidente. Es importante destacar que las listas de acceso utilizan caracteres comodín (*), de forma completamente opuesta a cómo se usan en las máscaras de red de una dirección IP. La primera línea de la lista de acceso en el ejemplo anterior tiene como objetivo filtrar el rango 10.0.0.0/8. Esto implica que hay que fijar el primer octeto de la dirección y permitir cualquier patrón en los 3 octetos restantes. Esto se obtiene utilizando el patrón 0.255.255.255.

Existe otro tipo de listas de acceso, llamadas *extended*, que permiten también filtrar paquetes basándose en sus direcciones IP origen y destino, y varios otros parámetros específicos de protocolo, como por ejemplo los números de puerto de los protocolos de transporte. Este tipo de listas están numeradas de 100 a 199 y de 2000 a 2699. Cuando se utilizan para filtrar rutas, la parte relativa a la dirección origen se utiliza para buscar la coincidencia de la dirección destino de la ruta, y la parte de la dirección destino se utiliza para la máscara de red. Por ejemplo [3]:

```
router(config)# router bgp 60055
router(config-router)# neighbor 192.0.254.17 distribute-list 110 in
router(config-router)# exit
router(config)# access-list 110 deny ip 128.0.0.0 0.255.255.255 255.255.128.0 0.0.127.255
router(config)# access-list 110 permit ip any any
router(config)# exit
```

En el ejemplo anterior, la lista de acceso 110 filtra todos los anuncios de prefijos /17 y más largos dentro del rango 128.0.0.0/8. La dirección de red destino puede ser cualquier cosa que empiece con 128: el primer octeto de la máscara es 0 (lo que significa que debe coincidir exactamente); los otros 3 octetos son 255 (comodín). La parte de la máscara de la ruta coincide con todas las máscaras desde 255.255.128.0 (/17), 255.255.192.0 (/18) y sucesivamente, hasta 255.255.255.254 (/31) y 255.255.255.255 (/32).

prefix-lists

Las listas de tipo *prefix-list* realizan la misma tarea que las *distribute-list*, pero de una forma mucho más sencilla de entender.

Una *prefix-list* básicamente es una lista de acceso que permite implementar políticas de filtrado en base a prefijos. Una *prefix-list* está formada por una o varias entradas ordenadas, que se van recorriendo en búsqueda de una coincidencia. Cada entrada está configurada para permitir (*permit*) o denegar (*deny*) el prefijo de la entrada en caso de coincidencia.
Las *prefix-lists* – que normalmente son configuradas con un nombre que se utiliza para identificarlas posteriormente – se evalúan comenzando por la entrada con menor número de secuencia y siguiendo en orden ascendente, hasta encontrar una entrada que coincida. Cuando se produce una coincidencia, se aplica la condición de la entrada (*permit* o *deny*) y el resto de la lista no se evalúa. Si se aplica una *prefix-list* y no hay ninguna entrada que coincida, implícitamente se aplica al tráfico la condición *deny*.

A continuación mostramos un ejemplo simple de uso de una *prefix-list* para filtrar los anuncios recibidos por un vecino en BGP [3], permitiendo sólo prefijos /20 y más cortos de Clase A y B, y prefijos /24 y más cortos de Clase C:

```
router(config)# router bgp 60055
router(config-router)# neighbor 192.0.254.17 prefix-list infilter in
router(config-router)# exit
router(config)# ip prefix-list infilter description filtro de entrada
router(config)# ip prefix-list infilter seq 5 permit 0.0.0.0/1 le 20
router(config)# ip prefix-list infilter seq 10 permit 128.0.0.0/2 le 20
router(config)# ip prefix-list infilter seq 15 permit 192.0.0.0/3 le 24
router(config)# exit
```

El parámetro *le* sirve para indicar prefijos que son iguales o más cortos (menos bits en el prefijo, es decir, bloques de direcciones más grandes). También se pueden indicar prefijos iguales o más largos (más bits en el prefijo, por lo tanto, bloques de direcciones más pequeños) con el parámetro *ge*, o incluso indicar rangos de direcciones combinando *ge* y *le*. Los números de secuencia facilitan borrar o insertar líneas en una *prefix-list*.
No es posible usar en BGP *distribute-lists* y *prefix-lists* simultáneamente en filtros de entrada o salida con un mismo vecino, pero sí que puede utilizarse cualquiera de ellos con una *filter-list*.

route-maps

Los *route-maps* son un método de controlar y modificar la información de encaminamiento. El control y la modificación de la información de encaminamiento se realiza a través de la definición de una serie de condiciones para la redistribución desde un protocolo de encaminamiento a otro. El control de la información de encaminamiento puede también ocurrir antes de dicha información sea recibida por BGP o enviada a un vecino. Un *route-map* tiene el siguiente formato:

```
route-map ETIQUETA_MAPA [[permit | deny] | [NÚMERO_SECUENCIA]]
```

`ETIQUETA_MAPA` es simplemente un nombre que se le asigna al *route-map*. Se pueden definir múltiples instancias/entradas de un mismo *route-map*. El número de secuencia `NÚMERO_SECUENCIA` es una indicación de la posición que ocupa dicha entrada en la lista de *route-maps* configurados con el mismo nombre.

En el siguiente ejemplo, hay dos entradas definidas de un mismo *route-map*, con el nombre `MI_MAPA`. La primera entrada tiene un número de secuencia 10 y la segunda un número de secuencia 20:

```
route-map MI_MAPA permit 10
      (el primer conjunto de condiciones va aquí)
route-map MI_MAPA permit 20
      (el segundo conjunto de condiciones va aquí)
```

Cuando se aplica el *route-map* `MI_MAPA` se aplica rutas entrantes o salientes, se aplica el primer conjunto de condiciones (se aplica la entrada con menor número de secuencia, en este caso, 10). Si no se cumplen las condiciones. se procede a continuación con una entrada con mayor número de secuencia del *route-map*.

Cada entrada/instancia de un *route-map* está compuesta de una lista de comandos de configuración *match* y *set*. Los comandos *match* indican un criterio de coincidencia que ha de cumplirse y los comandos *set* establecen las acciones a realizar si se cumplen los criterios indicados por el *match*.

Por ejemplo, se puede definir un *route-map* que compruebe los anuncios de rutas salientes. Si se cumple que hay una coincidencia para la dirección IP 1.1.1.1, la métrica de ese anuncio se establece a 5:

```
match ip address 1.1.1.1
set metric 5
```

Si se cumplen los criterios de coincidencia del *match* de una entrada/instancia del *route-map* y ésta es de tipo *permit*, se produce una redistribución o control de las rutas, modificados tal y como indiquen las clausulas *set*. Después de esto, se deja de procesar el *route-map* (no se interpretan el resto de entradas/instancias del *route-map*).

Si se cumplen los criterios de coincidencia del *match* de una entrada/instancia del *route-map* y ésta es de tipo *deny*, no se redistribuye ni controla de ninguna forma la ruta, dejando de procesar el resto de entradas/instancias del *route-map*.

Si no se cumplen los criterios de coincidencia del *match* de una entrada/instancia del *route-map* y ésta es de tipo *permit* o *deny*, se pasa a procesar la siguiente entrada/instancia. Este proceso continúa hasta que haya una entrada que cumpla con los criterios del *match* (lo cual produciría que se dejase de procesar el resto de entradas del *route-map*) o que se acaben las entradas del *route-map*. Si se acaban las entradas sin que se haya dado una coincidencia. la ruta no se acepta ni reenvía.

A continuación se enumeran los principales comandos de tipo *match*:

- `match as-path FILTER_LIST`
  - Busca coincidencia en el camino AS definido por la lista de tipo *filter-list* de nombre `FILTER_LIST`.
- `match interface NOMBRE_INTERFAZ`
  - Busca coincidencia en el nombre de la interfaz por la que se accede al primer salto de una ruta.
- `match ip address LISTA_ACCESO`
  - Aplica como criterio de coincidencia el filtrado definido en la lista de acceso `LISTA_ACCESO` (que puede ser un número de 1 a 199 para las listas *standard*, un número de 1300 a 2699 para las listas *extended* o el nombre de la lista).
- `match ip address prefix-list NOMBRE_PREFIX_LIST`
  - Aplica como criterio de coincidencia el filtrado definido en la lista de tipo *prefix-list*, de nombre `NOMBRE_PREFIX_LIST`.
- `match ip next-hop DIR_IPv4`
  - Busca coincidencia en la dirección del siguiente salto de una ruta con la dirección IP `DIR_IPv4`.
- `match ip next-hop LISTA_ACCESO`
  - Aplica como criterio de coincidencia en el siguiente salto de la ruta el filtrado definido en la lista de acceso `LISTA_ACCESO` (que puede ser un número de 1 a 199 para las listas *standard*, un número de 1300 a 2699 para las listas *extended* o el nombre de la lista).
- `match ip next-hop prefix-list NOMBRE_PREFIX_LIST`
  - Aplica como criterio de coincidencia en el siguiente salto de la ruta el filtrado definido en la lista de tipo *prefix-list*, de nombre `NOMBRE_PREFIX_LIST`.
- `match origin ORIGEN_BGP`
  - Busca coincidencia en el origen BGP de la ruta. `ORIGEN_BGP` puede ser: `egp` (para rutas originadas por un EGP remoto), `igp` (para rutas aprendidas por IGP local en el AS inicial) o `incomplete`.
- `match peer DIR_IPv4`
  - Busca coincidencia en la dirección IP (`DIR_IPv4`) en peer a través del cual hemos aprendido una ruta. `DIR_IPv4` puede ser también `local` para indicar rutas aprendidas localmente (rutas estáticas o redistribuidas localmente).
- `match community COMUNIDAD_BGP`
  - Busca coincidencia en la etiqueta de comunidad BGP (`COMUNIDAD_BGP`).

A continuación se enumeran los posibles comandos de tipo *set*:

- `set local-preference LOCAL_PREF`
  - Establece el valor del atributo *Local Preference* de la ruta BGP a `LOCAL_PREF`.
- `set ip next-hop DIR_IPv4`
  - Establece el valor de siguiente salto de la ruta a `DIR_IPv4`.
- `set ip next-hop DIR_IPv4`
  - Establece el valor de siguiente salto de la ruta a `DIR_IPv4`.
- `set as-path prepend NUMERO_AS`
  - Hace *prepend* del `NUMERO_AS` en el AS-PATH.
- `set as-path prepend NUMERO_AS`
  - Hace *prepend* del `NUMERO_AS` en el AS-PATH.
- `set origin ORIGEN_BGP`
  - Establece el origen de la ruta BGP a `ORIGEN_BGP`. `ORIGEN_BGP` puede ser: `egp`, `igp` o `incomplete`.

- `set weight PESO`
  - Establece el atributo *weight* de la ruta BGP al valor `PESO` (valor entre 0 y 4294967295).
- `set community NÚMERO_COMUNIDAD_BGP`
  - Establece el atributo *community* al valor `NÚMERO_COMUNIDAD_BGP`.

A continuación incluimos un ejemplo simple de utilización de *route-maps*:

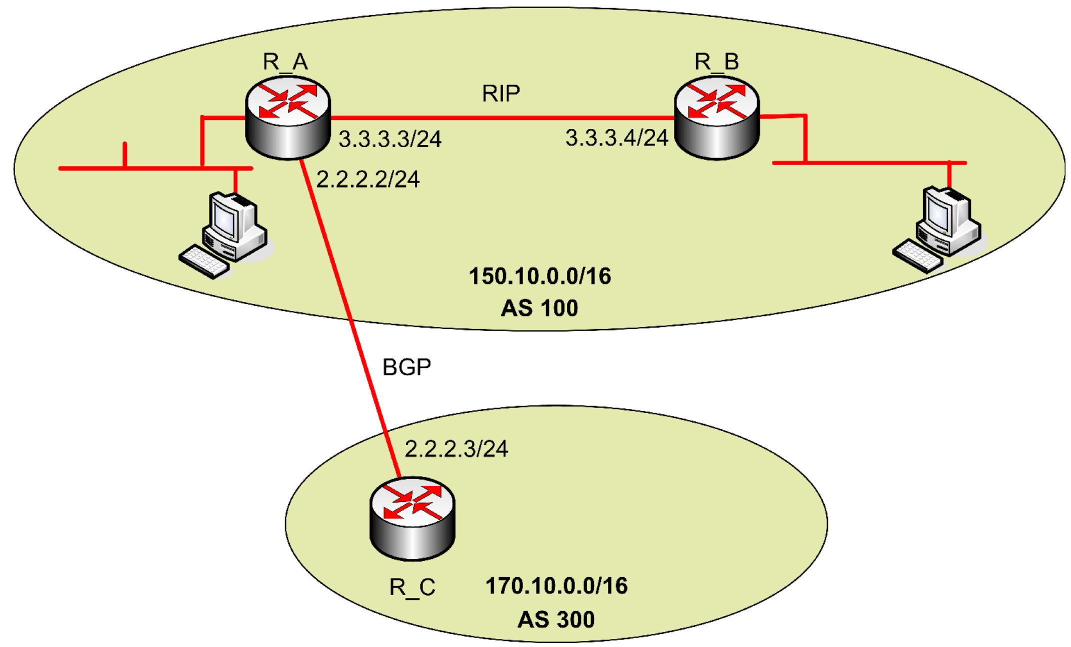


Figura 4: Escenario ejemplo de uso de route-maps

Los routers R_A y R_B pertenecientes al AS 100 ejecutan RIP y R_A y R_C hablan BGP entre ellos. El router R_A recibe anuncios de rutas a través de BGP y los redistribuye utilizando RIP dentro de su AS. Suponga que R_A quiere redistribuir a R_B las rutas hacia 170.10.0.0/16 con una métrica de 2 y el resto de rutas con métrica 5. Para ello, se podría usar la siguiente configuración en el router R_A:

```
R_A# configure terminal
R_A(config)# router rip
R_A(config-router)# network 3.3.3.0/24
R_A(config-router)# network 2.2.2.0/24
R_A(config-router)# network 150.10.0.0/16
R_A(config-router)# redistribute bgp 100 route-map SETMETRIC
R_A(config-router)# exit
R_A(config)# router bgp 100
R_A(config-router)# neighbor 2.2.2.3 remote-as 300
R_A(config-router)# network 150.10.0.0/16
R_A(config-router)# exit
R_A(config)# route-map SETMETRIC permit 10
R_A(config-route-map)# match ip address prefix-list prefijo
R_A(config-route-map)# set metric 2
R_A(config-route-map)# exit
R_A(config)# route-map SETMETRIC permit 20
R_A(config-route-map)# set metric 5
R_A(config-route-map)# exit
R_A(config)# ip prefix-list prefijo seq 5 permit 170.10.0.0/16
```

En el ejemplo, si el router R_A recibe un anuncio de ruta hacia 170.10.0.0/16, la ruta se redistribuye mediante RIP dentro del AS 100 con una métrica igual a 2 y se sale del *route-map*. Si no hay coincidencia, se procesa la siguiente entra del *route-map*. que indica que cualquier otra ruta recibida se redistribuye con métrica 5. Si se hubiera dado la posibilidad de que alguna ruta no coincidiera con ninguna de las entradas del *route-map*, esa ruta se hubiera descartado, no siendo redistribuida a la tabla RIP.

4. COMANDOS DISPONIBLES CUANDO SE ACCEDE POR SSH

Esta sección incluye los comandos básicos de configuración que se pueden realizar a través de la consola de configuración accesible mediante un *ssh* al router. Al igual que para acceder por *telnet*, debe configurar en su PC una dirección IP que le permita tener conectividad con el router WRT54GS/GL (la dirección dependerá de la interfaz de red del router que vaya a utilizar para acceder desde el PC). Los parámetros de acceso necesarios son:

- Usuario: alumno
- Contraseña: alumno13

4.1 Configuración de la interfaz inalámbrica

Los parámetros de configuración de la interfaz inalámbrica (interfaz `wlan0`) se indican en el fichero `/etc/config/wireless`:

```
config wifi-device  wl0
        option type     broadcom
        option channel  5

        # REMOVE THIS LINE TO ENABLE WIFI:
        option disabled 1

config wifi-iface
        option device   wl0
        #option network wl0
        option mode     adhoc
        option ssid     practicas_IT.UC3M
        option encryption none
```

Por defecto la interfaz inalámbrica está deshabilitada. Para habilitarla debe borrar la línea `option disabled 1`. Cada vez que reinicie el router, éste arrancará con su configuración por defecto (interfaz inalámbrica deshabilitada). La mayoría de los parámetros del fichero son autoexplicativos. Los más importantes son los siguientes (puede consultar la lista completa en [4]):

- `mode`: especifica el modo de operación de la tarjeta (`ap`: modo punto de acceso, sta: modo estación, `adhoc`: modo ad-hoc y `monitor`: modo monitor)
- `ssid`: especifica el SSID de la red
- `channel`: especifica el canal (frecuencia de operación)
- `encryption`: especifica el modo de cifrado (`wep`: modo WEP, `psk`: modo WPA-PSK y `psk2`: modo WPA2-PSK).
- `key`: especifica la clave utilizada (en modo WEP o WPA-PSK).

Para configurar la tarjeta de un modo determinado, genere el fichero de configuración adecuado y utilice el comando `wifi_uc3m up` a continuación. La interfaz wireless del router es sensible a cambios, por lo que es posible que no pueda realizar ciertos cambios sin reiniciar el router antes y partir de nuevo de la configuración por defecto.

Algunos aspectos del comportamiento de la interfaz inalámbrica se pueden modificar también utilizando los comandos de las *wireless-tools* (`iwconfig` e `iwlist`). Además, también existen herramientas propias del hardware de los routers: `wl` y `wlc` (por ejemplo, el comando `wl radio off` apaga la interfaz). Pruebe también a emplear dichos comandos para realizar ciertas configuraciones sin necesidad de emplear el fichero de configuración ni/o reiniciar el router.

4.2 Activación del demonio SNMP

Los routers disponen también de un demonio SNMP que implementa la funcionalidad de agente SNMP. Por defecto se encuentra deshabilitado. Se puede activar mediante el comando `start_snmpd`.

4.3 Desactivación de los demonios de encaminamiento

Si se desea parar los demonios de encaminamiento, esto se puede hacer mediante la ejecución del comando `stop_routing`.

Referencias

[1] Manual de Quagga, http://www.quagga.net/docs.php
[2] BGP Case Studies: AS Regular Expression http://www.cisco.com/warp/public/459/bgp-toc.html#asregexp
[3] Iljitsch van Beijnum, "BGP. Building Reliable Networks with the Border Gateway Protocol" (L/D 004.738.5.057.4 BEI).
[4] Open Wrt Wiki: Wireless Configuration. http://wiki.openwrt.org/doc/uci/wireless